



1401 Lawrence Street, Suite 2300, Denver, CO 80202 • (303) 572-9300

May 26, 2020

Michael J. Waters
312.463.6212
312.873.2918 Fax
mwaters@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of a Data Security Incident

Dear Mr. Karberg:

We represent Compass Health, Inc., d/b/a Compass Health Network (“Compass”) in connection with a recent incident that may have impacted the personal information of three (3) Maryland residents, and provide this notice on behalf of Compass pursuant to MD. CODE ANN., COM. LAW § 14-3504(h). We will supplement this letter, if necessary, with any new significant facts discovered subsequent to its submission. While Compass is notifying you of this incident, Compass does not waive any rights or defenses relating to the incident or this notice.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On or around March 20, 2020, PaperlessPay Corporation (“PaperlessPay”) notified Compass of a security incident that it recently experienced. Compass contracts with PaperlessPay for the provision of online bi-weekly paystubs and W-2 tax forms. According to PaperlessPay, on February 19, 2020, the Department of Homeland Security (“DHS”) contacted PaperlessPay and notified it that someone was purporting to sell access to PaperlessPay’s client database on the dark web. PaperlessPay shut down its web server and SQL server to prevent unauthorized access. PaperlessPay worked with the Federal Bureau of Investigation (“FBI”) and retained a cybersecurity firm to conduct a forensic investigation. The investigation revealed that someone accessed PaperlessPay’s SQL server on February 18, 2020. Compass and PaperlessPay worked together to obtain additional information concerning the incident, including what, if any information the threat-actor may have acquired.

At this point, Compass is not aware of an unauthorized access or acquisition of its employees’ personal information or that any of the information has been misused. However, PaperlessPay

polsinelli.com

Atlanta	Boston	Chicago	Dallas	Denver	Houston	Kansas City	Los Angeles	Miami	Nashville	New York
Phoenix	St. Louis	San Francisco	Seattle	Silicon Valley	Washington, D.C.	Wilmington				

Polsinelli PC, Polsinelli LLP in California

May 26, 2020

Page 2

could not definitely rule out the possibility that someone accessed or acquired Compass' employees' personal information. Accordingly, Compass is notifying the potentially impacted employees and arranged for complementary identity theft protection services for the employees.

NUMBER OF MARYLAND RESIDENTS AFFECTED

Compass determined that the incident potentially impacted three (3) Maryland residents. Compass is notifying the potentially impacted Maryland residents of the incident by letter later today. Enclosed is a copy of the notice that Compass is sending to the impacted individuals.

STEPS TAKEN RELATING TO THE INCIDENT

Upon becoming aware of the incident, Compass promptly investigated the incident to determine what, if any, personal information a third party might have acquired during the incident. Compass is also providing complimentary identity theft protection services to the impacted individuals through Experian.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,



Michael J. Waters

Enclosure